Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/BR05/000030

International filing date: 10 March 2005 (10.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: BR
Number: PI0400265-2
Filing date: 10 March 2004 (10.03.2004)

Date of receipt at the International Bureau: 19 April 2005 (19.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT / BR 2005/000030

REPUBLICA FEDERATIVA DO BRASIL
Ministério do Desenvolvimento, da Indústria e Comércio Exterior.
Instituto Nacional da Propriedade Industrial
Diretoria de Patentes

CÓPIA OFICIAL

PARA EFEITO DE REIVINDICAÇÃO DE PRIORIDADE

O documento anexo é a cópia fiel de um Pedido de Patente de Invenção. Regularmente depositado no Instituto Nacional da Propriedade Industrial, sob Número PI 0400265-2 de 10/03/2004.

Rio de Janeiro, 18 de Março de 2005.

Oscar Paulo Bueno
Chefe do Nucad
Mat: 0449117

Protocolo

Número (21)

DEPÓSITO

Pedido de Patente ou de Certificado de Adição

PI0400265-2

depósito / /

a de depósito)

Ao Instituto Nacional da Propriedade Industrial:

O requerente solicita a concessão de uma patente na natureza e nas condições abaixo indicadas:

1. Depositante (71):

1.1 Nome: **AUTOMATOS TECNOLOGIA DE INFORMAÇÃO LTDA**

1.2 Qualificação: 1.3 CGC/CPF: **02632835000190**

1.4 Endereço completo: **PRAÇA FLORIANO, 19, 22° ANDAR, SALA 2201 - PARTE -CENTRO - RIO DE JANEIRO - RJ**

1.5 Telefone: **2544-3977**

FAX:

☐ continua em folha anexa

2. Natureza:

☒ 2.1 Invenção ☐ 2.1.1. Certificado de Adição ☐ 2.2 Modelo de Utilidade

Escreva, obrigatoriamente e por extenso, a Natureza desejada: **INVENÇÃO**

3. Título da Invenção, do Modelo de Utilidade ou do Certificado de Adição (54):

SISTEMA DE CONTROLE DE ACESSO A SERVIÇOS DE

☒ continua em folha anexa

4. Pedido de Divisão do pedido n°. , de .

5. Prioridade Interna - O depositante reivindica a seguinte prioridade:

N° de depósito Data de Depósito **(66)**

6. Prioridade - o depositante reivindica a(s) seguinte(s) prioridade(s):

País ou organização de origem	Número do depósito	Data do depósito

☐ continua em folha anexa

7. Inventor (72):

☐ Assinale aqui se o(s) mesmo(s) requer(em) a não divulgação de seu(s) nome(s) (art. 6° § 4° da LPI e item 1.1 do Ato Normativo n° 127/97)

7.1 Nome: **AGOSTINHO DE ARRUDA VILLELA**

7.2 Qualificação: **Engenheiro**

7.3 Endereço: **RUA BARÃO DA TORRE, 260/203 - IPANEMA - RIO DE JANEIRO - RJ**

CONTINUAÇÃO -Título da invenção, do modelo de utilidade ou do certificado de adição (54) :

informação baseado em assinatura de hardware e software do dispositivo solicitante.

7.4 CEP: 7.5 Telefone

☐ continua em folha anexa

8. Declaração na forma do item 3.2 do Ato Normativo nº 127/97:

☐ em anexo

9. Declaração de divulgação anterior não prejudicial (Período de graça):
(art. 12 da LPI e item 2 do Ato Normativo nº 127/97):

☐ em anexo

10. Procurador (74):
10.1 Nome **MARCO TÚLIO DE BARROS E CASTRO** 10ABIRJ-112.979
CPF/CGC: **08167863727**
10.2 Endereço: **AV. RIO BRANCO, 109/903 - CENTRO - RIO DE JANEIRO - RJ**
10.3 CEP: **20040004** 10.4 Telefone **2232-6776**

11. Documentos anexados (assinale e indique também o número de folhas):
(Deverá ser indicado o nº total de somente uma das vias de cada documento)

☒	11.1 Guia de recolhimento	**01** fls.	☒	11.5 Relatório descritivo	**09** fls.
☒	11.2 Procuração	**01** fls.	☒	11.6 Reivindicações	**05** fls.
☐	11.3 Documentos de prioridade	fls.	☐	11.7 Desenhos	**03** fls.
☐	11.4 Doc. de contrato de Trabalho	fls.	☐	11.8 Resumo	**01** fls.
☐	11.9 Outros (especificar): CNPJ e QUARTA ALTERAÇÃO CONTRATUAL				**05** fls.
	11.10 Total de folhas anexadas:				**25** fls;

12. Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras

10.03.2004
Local e Data

Assinatura e Carimbo

SISTEMA DE CONTROLE DE ACESSO A SERVIÇOS DE INFORMAÇÃO BASEADO EM ASSINATURA DE HARDWARE E SOFTWARE DO DISPOSITIVO SOLICITANTE

A presente Invenção refere-se a dispositivos computacionais ou com capacidade computacional para identificação e autorização de acesso.

Mais particularmente, a presente Invenção é particularmente aplicável no acesso a informações sensíveis e confidenciais tais como acessos via Internet a contas bancárias, acesso seguro a páginas eletrônicas para transações comerciais (*e-commerce*), acesso a intranet de uso confidencial em ambientes empresariais, etc.

ANTECEDENTES DA INVENÇÃO

São conhecidos diversos dispositivos e configurações de segurança relativos a acessos e operações eletrônicas e via internet. A necessidade de segurança tem que ser constantemente revista em função do avanço nos recursos utilizados para burlar sistemas e fraudar acessos eletrônicos a *internet banking* e compras por meios eletrônicos. Em países como os EUA, o rigor na coibição de atos criminosos praticados por *hackers* dá a exata dimensão da importância deste crescente ramo de atividade comercial. Muitas operações *online* ou via internet contam com níveis de segurança que se baseiam na maior complexidade das formas de acesso a serviços eletrônicos de caráter particular ou que sejam confidenciais. Entretanto, esta maior complexidade acaba por causar uma dificuldade ao usuário legitimamente habilitado em acessar tais serviços e, portanto, a perda de comodidade do usuário, conjugada com outros fatores, gerou um crescimento aquém do esperado das operações eletrônicas.

Outros sistemas de segurança aparentemente mais rigorosos tais como os dos auto-serviços bancários são um exemplo do que foi acima exposto. Serviços de acesso doméstico atuam de maneira unilateral como se apenas o usuário enxergasse o serviço. O reconhecimento a partir do usuário mostra-se

bastante limitativo em função da susceptibilidade do rastreamento de senhas a partir do acesso de um usuário qualquer. Esta forma de correspondência unívoca facilita a fraude por parte dos hackers seja por meio de clonagem das senhas, seja por clonagem dos endereços acessados.

Como exemplo da técnica, o documento irlandês 83221 refere-se a meios de identificação única de computadores e sistemas. A Invenção, em contraste, é capaz de criar assinaturas que identificam um dispositivo a partir de informações lógicas e, em conjunto com uma estrutura unívoca e processos atinentes que a integram, propor um sistema que complementa ou substitui esquemas tradicionais de autenticação. Ainda que assinaturas ou a idéia de se usar esquemas de positivação estendida para dispositivos computacionais existam há bastante tempo, a unidade de Invenção compreende o processo, i.e., arquitetura agente/servidor para complementar ou substituir esquemas de autenticação.

Assim, o que é reivindicado no documento 83221 compreende a criação de uma assinatura única para um dispositivo (onde um dispositivo representa um processador ou um conjunto de processadores formando uma rede) baseada nas distribuições estatísticas de tempos de resposta e outras métricas de identificação física dos mesmos, com propósitos que podem ou não servir a esquemas convencionais de autenticação. Algumas formas lógicas também são utilizadas no processo de identificação proposto neste documento de patente, porém ao contrário da Invenção, estas formas lógicas são usadas de maneira complementar às físicas, não sendo suficientes para criar a identificação única de um dispositivo proposta no documento 83221. Ainda que a partir do documento 83221 seja possível criar ou complementar esquemas de autenticação, não é objetivada, nem o seu conteúdo contemplaria, diretamente, a criação de um processo assemelhado. O que se objetiva no documento 83221 é criar, ou pretender criar, uma identificação única para um dispositivo.

Este também é o caso da publicação da Microsoft®: PRODUCT ACTIVATION FOR WINDOWS XP-TECHNICAL MARKET BULLETIN. Esta

publicação versa sobre formas de validação de programas WINDOWS XP em equipamentos de maneira a evitar a cópia ilegal (pirataria) ou mesmo a aquisição de produtos fraudulentos. As configurações dispostas para tanto também são de caráter unívoco, de alguma complexidade para o usuário comum, o qual seria inibido de praticar atos fraudulentos.

DESCRIÇÃO SUMÁRIA DA INVENÇÃO

A presente Invenção é uma tecnologia utilizada para aumentar substancialmente a segurança num processo de autenticação para acessar uma página de Internet, Intranet, ou qualquer outro tipo de servidor computacional ou serviço de informática que possa requerer autenticação segura. Qualquer um destes serviços será citado doravante como "SERVIÇO". A autenticação passa a incluir um processo conjugado ao perfil de configuração de hardware e software de um dispositivo, perfazendo uma assinatura deste dispositivo. Esta assinatura será referenciada doravante como "ASSINATURA".

Sempre que um usuário tentar acessar um SERVIÇO que esteja utilizando a Invenção para autenticação, a ASSINATURA decorrente da configuração do dispositivo de onde ele está tentando acessar o SERVIÇO é verificada e comparada com uma lista de ASSINATURAS de dispositivos autorizados. Se a ASSINATURA do dispositivo corrente corresponder exatamente a uma das ASSINATURAS previamente cadastradas, o usuário conseguirá acessar o SERVIÇO. Caso contrário, ele será submetido à positivação estendida ou terá acesso negado, dependendo das opções de segurança previamente escolhidas. No caso de ser submetido à positivação estendida, se a identificação for bem sucedida, ele conseguirá acessar o SERVIÇO e poderá, opcionalmente, incluir o dispositivo presente na lista das ASSINATURAS cadastradas para a sua conta. Se a identificação não for bem sucedida, o usuário não conseguirá acessar a conta.

A Invenção pode ser usada como um processo de autenticação complementar a outro processo de autenticação pré-existente (autenticação

por identificador de usuário e senha, por exemplo) de forma a aprimorar a sua segurança. Alternativamente, a Invenção também pode ser utilizada de forma a substituir um processo de autenticação. Isto pode ser usado, tipicamente, no caso de aplicações menos sensíveis, tal como a identificação perante um portal ou provedor de acesso.

Cabe salientar que a Invenção é capaz de realizar esta identificação sem a necessidade de instalação de qualquer outro componente adicional de hardware ou software, tais como cartões de identificação (*smart cards*), placas de identificação, etc. Portanto, a Invenção permite o reconhecimento da ASSINATURA de um dispositivo simplesmente a partir de seus componentes de hardware e software usuais instalados.

Um maior detalhamento será proporcionado em termos de uma das aplicações que podem ser atribuídas a presente Invenção, entretanto esta descrição não é limitativa do escopo presentemente reivindicado.

DESCRIÇÃO DAS FIGURAS

A Figura 1 é um diagrama que ilustra o funcionamento básico da presente Invenção;

A Figura 2 é um diagrama que ilustra o processo de remoção de ASSINATURAS;

A Figura 3 é um diagrama representativo do processo de desativação de uso do sistema por um usuário.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Arquitetura do sistema

A presente Invenção foi concebida para operar em um ambiente computacional distribuído que pode ser implementado através da Internet ou em uma rede computacional interna. Ele é constituído de três componentes básicos:

a) Um Agente Coletor;

b) Um Servidor de Autenticação;

c) Um Serviço disponível via rede que requeira autenticação.

O Agente Coletor é um programa que permite inventariar informações de hardware e software de um dispositivo. Ele é a peça chave para obter os dados que irão compor a ASSINATURA do dispositivo. O Agente Coletor precisa estar instalado ou ser baixado e instalado no dispositivo (preferencialmente, usando técnicas de distribuição via *Web* que baixam um programa e o executam num único passo, por exemplo, *ActiveX* ou *plug-in* de *browser*), através da Internet ou de uma rede interna, para dar início ao processo de identificação de ASSINATURA.

O Servidor de Autenticação é um servidor computacional que recebe a ASSINATURA coletada por um Agente Coletor, confronta-a com um conjunto de ASSINATURAS autorizadas e autoriza ou não uma tentativa de acesso a um SERVIÇO. O Servidor de Autenticação precisa estar conectado numa rede interna ou através da Internet ao dispositivo sujeito a autenticação de ASSINATURA para que o processo de autenticação da Invenção consiga funcionar. Ele é, portanto, um sistema de autenticação online.

O Servidor de Autenticação tem uma função tanto interativa como de armazenamento. Ele interage com o Agente Coletor e o SERVIÇO provendo a autenticação do acesso. Além disto, ele funciona como um repositório das ASSINATURAS cadastradas bem como do histórico de tentativas de acesso (bem sucedidas ou não) de cada usuário ao SERVIÇO.

O SERVIÇO é uma página de Internet, Intranet, ou qualquer outro tipo de servidor computacional ou serviço de informática que possa requerer autenticação segura. A Invenção pode atuar em complementação a outras formas de autenticação ou procedimento de segurança já utilizado pelo SERVIÇO, como uma pré-identificação. Por exemplo, pode ser usada para impedir o uso do SERVIÇO a partir de um dispositivo cuja ASSINATURA não seja reconhecida e cadastrada, mesmo que uma outra pré-identificação consiga ser feita de forma bem sucedida por outros processos de uso

concomitante (impedir o acesso mesmo que um usuário preencha um identificador e uma senha de acesso corretos).

Modo de funcionamento

O funcionamento do sistema da presente Invenção é exemplificado pelos passos descritos abaixo:

1) Um usuário tenta acessar o SERVIÇO submetido à autenticação da Invenção. Visto que a mesma pode conviver com outras formas de autenticação, o usuário poderá se submeter a este tipo de identificação ou segurança complementar, como se fosse uma pré-identificação, caso seja necessário. Exemplos típicos de processos de pré-identificação e segurança complementar são: preenchimento de um identificador de conta e senha, verificação de faixas de endereços IP autorizados a acessar o SERVIÇO, respostas a perguntas, sistemas de proteção contra "robôs de software", etc.

2) Se o usuário ainda não registrou a ASSINATURA de dispositivo algum perante a Invenção, o usuário será levado a uma página ou janela explicando o funcionamento da Invenção e explicando que ele será submetido a um processo de cadastramento logo em seguida.

a. Este passo pode ser implementado de forma a ser opcional, caso o provedor do SERVIÇO queira proporcionar ao usuário a opção de acessar o SERVIÇO usando ou não a Invenção, sob sua própria responsabilidade. Neste caso, o usuário poderá também tomar a iniciativa de desativar ou reativar o uso da Invenção quando desejado. Para reativar a mesma, o usuário deverá se identificar de alguma forma (por meio de identificador e senha, resposta a perguntas, etc). Recomenda-se só permitir desativar a Invenção a partir do dispositivo que possui a ASSINATURA ativa mais antiga cadastrada na conta do usuário já que esta ASSINATURA é geralmente considerada a mais confiável.

3) Uma vez que o usuário concorde com o uso da Invenção, ele deverá permitir que o Agente Coletor seja baixado e instalado no seu dispositivo, a não ser que o Agente Coletor já tenha sido instalado previamente.

Este passo deverá ser repetido para cada dispositivo que precise ser submetido ao processo de autenticação da Invenção.

4) Uma vez que o Agente Coletor esteja instalado no dispositivo do usuário, a Invenção irá identificar a sua ASSINATURA e submetê-la ao cadastro de uso do SERVIÇO. Tipicamente, o primeiro cadastramento não requer autenticação mais rigorosa.

A ASSINATURA é composta a partir de dados coletados dos componentes de hardware e software do dispositivo. Ela irá identificar o dispositivo perante a Invenção sem a necessidade de instalação de qualquer outro dispositivo suplementar, tal como um cartão de identificação (*smart card*).

A identificação de um dispositivo é feita por meio da detecção e identificação de componentes essenciais de hardware e software do dispositivo. A Invenção admite que alguns destes itens possam sofrer alterações incrementais sem que a ASSINATURA do dispositivo seja modificada. Entretanto, caso sejam efetuadas alterações profundas, a ASSINATURA será alterada. Isto significa que o dispositivo passará a ser considerado como sendo outro, e não será reconhecido pelos SERVIÇOS outrora acessados. Neste caso, o usuário deverá recadastrar a nova ASSINATURA perante a Invenção. Cabe esclarecer também que alterações de componentes que não são considerados como essenciais podem ser feitas sem afetar a ASSINATURA.

A ASSINATURA é composta de parcelas (*hashes*) concatenadas de informações oriundas dos componentes de hardware e software. Ela não pode ser revertida para recompor as informações originais que foram usadas para criá-la, preservando, assim, a privacidade e segurança do usuário. É recomendável que a cada transação, as *hashes* sejam concatenadas de forma diferente e submetidas a várias camadas de criptografia. Este procedimento protege ainda mais contra qualquer tentativa de se interceptar a comunicação entre o dispositivo do usuário e o Servidor de Autenticação e se tentar, pela

simples reprodução dos dados transmitidos, se fazer passar por este dispositivo.

5) Se o usuário acessar o SERVIÇO a partir de um dispositivo não cadastrado (desde que haja pelo menos um dispositivo previamente cadastrado), a Invenção apenas permitirá o acesso após o uso de positivação estendida (i.e. perguntas específicas além do par usuário/senha). Se confirmadas as respostas, o usuário terá o acesso ao SERVIÇO concedido, com a opção de cadastrar (ou não) a ASSINATURA do novo dispositivo, conforme a configuração previamente escolhida. Caso a identificação falhe, ele não conseguirá acessar o SERVIÇO.

a. Opcionalmente, caso o usuário já tenha atingido uma determinada quantidade de ASSINATURAS cadastradas (definida conforme a implementação), ele poderá escolher se deseja limitar o número de ASSINATURAS a esta quantidade ou não. Alternativamente, pode se limitar o conjunto de assinaturas de forma a se criar um grupo fechado de dispositivos que podem acessar um SERVIÇO através de uma determinada conta de usuário. Estas opções podem ser implementadas de forma a se tornar mandatórias, ou seja, o usuário só conseguirá cadastrar ASSINATURAS na sua conta até um número máximo ou apenas de dispositivos pertencentes a um determinado conjunto.

b. Mesmo para o caso em que não se admita o cadastro de ASSINATURAS adicionais, é possível, ainda assim, opcionalmente, se acessar o SERVIÇO através de um dispositivo não cadastrado mediante o uso de positivação estendida. De qualquer forma, a ASSINATURA deste dispositivo NÃO poderá ser adicionada ao conjunto de ASSINATURAS já existente. Nesta situação, o acesso ao SERVIÇO, a partir deste dispositivo, é efetuado estritamente sob caráter "avulso" e provisório.

c. Opcionalmente, também é possível se estipular o número máximo de vezes que uma ASSINATURA pode estar presente para diferentes usuários do serviço. Este número máximo pode, inclusive, ser igual a zero. Nesta

situação, o dispositivo em questão é considerado como "malicioso" e passa a fazer parte de uma lista de exclusão contendo dispositivos que não estão autorizados a se autenticar perante a Invenção.

6) Sempre que julgar necessário, o usuário poderá remover as ASSINATURAS cadastradas na sua conta. Recomenda-se que o processo de remoção de ASSINATURAS seja sempre feito a partir de um dispositivo considerado mais seguro ou confiável, o qual é, tipicamente, um dispositivo cadastrado na conta há mais tempo. Desta forma, o usuário só poderá remover uma dada assinatura se estiver operando a partir de um dispositivo cuja ASSINATURA tenha sido cadastrada ANTES da ASSINATURA que está sendo removida. Recomenda-se também que a ASSINATURA de cadastro mais antiga de todas só possa ser removida a partir do próprio dispositivo da mesma.

7) Uma vez que o usuário passe a acessar a página regularmente por meio da Invenção, a mesma estará capacitada a prover informações sobre todos os acesso ou tentativas de acesso à conta do usuário. Este histórico será armazenado mesmo que o usuário decida desativar, ainda que temporariamente, a utilização do sistema da presente Invenção.

REIVINDICAÇÕES

1- Sistema de identificação de dispositivos e controle de acesso de usuários e dispositivos a serviços de informação, sem a necessidade de uso de biometria ou dispositivos como *smart cards*, baseado na geração de uma ASSINATURA para cada dispositivo e em processos autorizativos **caracterizado** por compreender:

Coleta de dados dos dispositivos a partir da execução de um Agente Coletor para a geração de uma ASSINATURA, onde o Agente Coletor pode estar integrado ao processo original de acesso a um SERVIÇO; o Agente Coletor processa dados de configurações de hardware e software coletados do dispositivo, e disponibiliza a ASSINATURA através do uso de hashes que se alteram a cada acesso; e

Envio de uma ASSINATURA irreversível do dispositivo, utilizando várias camadas de criptografia no envio da mesma para o Servidor de Autenticação.

2-Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a criação e envio de uma ASSINATURA compreende uma das etapas de uma arquitetura *("framework")* de processos autorizativos a fim de permitir (ou negar) o acesso do dispositivo aos SERVIÇOS, em que:

i. o acesso a um Servidor de Autenticação que recebe e verifica a ASSINATURA, confrontando-a com o repositório de ASSINATURAS cadastradas;

ii. o Servidor de Autenticação é capaz de, baseado em configurações do usuário ou do provedor do SERVIÇO, conforme o caso:

a) identificar se o dispositivo foi incluído em uma lista de exclusão (*blacklist*) para fins de cadastramento e/ou acesso ao SERVIÇO;

b) criar um grupo fechado de dispositivos (*closed group*) que pode acessar o SERVIÇO, impedindo o acesso ao SERVIÇO a partir de outros dispositivos;

c) criar um grupo fechado de dispositivos (*closed group*) impedindo o cadastramento de dispositivos adicionais;

d) permitir um número máximo de cadastramentos para um dispositivo único, onde a situação descrita no item "a" acima corresponde a um número máximo igual a zero;

e) descadastrar um dispositivo;

f) cadastrar dispositivos adicionais;

iii. o Servidor de Autenticação é capaz de, independentemente de configurações do usuário ou provedor do SERVIÇO:

a) permitir modificações incrementais nas configurações de hardware e software de um dispositivo já cadastrado sem que as mesmas impossibilitem (I) o acesso do mesmo ao SERVIÇO; ou (II) o reconhecimento de um dispositivo incluído numa lista de exclusão;

b) uma vez concedido o acesso, atualizar as ASSINATURAS modificadas nos termos do item anterior;

c) submeter um dispositivo já cadastrado que tenha sofrido modificações substanciais nas suas configurações de hardware e software ao mesmo tratamento conferido a dispositivos não cadastrados;

d) registrar todos os acessos ou tentativas de acesso de um dispositivo ao SERVIÇO, mantendo o registro mesmo na hipótese de desativação do uso ou descadastramento de um dispositivo;

e) impedir que um usuário, a partir de um dispositivo hierarquicamente inferior, *i.e.*, cujo cadastramento tenha ocorrido por último, descadastre um dispositivo hierarquicamente superior, *i.e.*, cujo cadastramento tenha ocorrido primeiro;

f) impedir que um usuário, a partir de um dispositivo hierarquicamente inferior, *i.e.*, cujo cadastramento tenha ocorrido por último, desabilite a Invenção;

iv. Para o primeiro acesso de um usuário previamente identificado, onde não há dispositivos cadastrados:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) o Servidor de Autenticação verifica o parâmetro listado no item ***ii. "a"***;

c) o Servidor de Autenticação verifica os parâmetros listados nos itens ***ii. "c"*** e ***"d"***.;

d) com base na anuência do usuário, a ASSINATURA é cadastrada, o dispositivo é incluído no grupo autorizado e o usuário tem acesso ao SERVIÇO;

e) se o item ***"b"*** acima não for satisfeito, o acesso ao SERVIÇO é negado;

v. Para os acessos subseqüentes de um usuário previamente identificado a partir de um dispositivo já cadastrado:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) o Servidor de Autenticação reconhece a ASSINATURA, autorizando o acesso ao SERVIÇO em caso de sucesso;

vi. Para os acessos subseqüentes de um usuário a partir de um dispositivo não cadastrado:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) o Servidor de Autenticação verifica os parâmetros listados no item ***ii "a"*** e ***"b"***; e,

c) aplicam-se as etapas descritas nos itens ***iv "c"*** e ***"d"***;

d) se o item ***"b"*** acima não for satisfeito, o acesso ao SERVIÇO é negado.

3-Uso de um sistema de identificação de dispositivos para controle de acesso de usuários e dispositivos a serviços de informação sem a necessidade

de uso de biometria, ou dispositivos como *smart cards*, de acordo com as reivindicações 1 e 2, **caracterizado** por compreender:

Coleta de dados dos dispositivos a partir da execução de um Agente Coletor para a geração de uma ASSINATURA digital, onde o Agente Coletor pode estar integrado ao processo original de acesso a um SERVIÇO. O Agente Coletor processa dados de configurações de hardware e software coletados do dispositivo, e disponibiliza a assinatura através do uso de hashes que se alteram a cada acesso; e

Criação e envio de uma ASSINATURA irreversível do dispositivo, utilizando várias camadas de criptografia no envio da mesma para o Servidor de Autenticação.

4- Uso de um sistema de identificação de dispositivos para controle de acesso de usuários e dispositivos a serviços de informação sem a necessidade de uso de biometria, ou dispositivos como smart cards, de acordo com a reivindicação 3, **caracterizado** por compreender:

i. o acesso a um Servidor de Autenticação que recebe e verifica a ASSINATURA, confrontando-a com o repositório de assinaturas cadastradas;

ii. o Servidor de Autenticação é capaz de, baseado em configurações do usuário ou do provedor do SERVIÇO, conforme o caso:

a) identificar se o dispositivo foi incluído em uma lista de exclusão (*blacklist*) para fins de cadastramento e/ou acesso ao SERVIÇO;

b) criar um grupo fechado de dispositivos (*closed group*) que pode acessar o SERVIÇO, negando o cadastro de outros dispositivos ou o acesso ao SERVIÇO a partir de outros dispositivos;

c) criar um grupo fechado de dispositivos (*closed group*) impedindo o cadastramento de máquinas adicionais;

d) permitir um número máximo de cadastramentos para um dispositivo único, onde a situação descrita no item "a" acima corresponde a um número máximo igual a zero;

e) descadastrar um dispositivo;

f) cadastrar dispositivos adicionais;

iii. o Servidor de Autenticação é capaz de, independentemente de configurações do usuário ou provedor do SERVIÇO:

a) permitir modificações incrementais nas configurações de hardware e software de um dispositivo já cadastrado sem que as mesmas impossibilitem (I) o acesso do mesmo ao SERVIÇO; ou (II) o reconhecimento de um dispositivo incluído numa lista de exclusão;

b) uma vez concedido o acesso, atualizar as ASSINATURAS modificadas nos termos do item anterior;

c) submeter um dispositivo já cadastrado que tenha sofrido modificações substanciais nas suas configurações de hardware e software ao mesmo tratamento conferido a dispositivos não cadastrados;

d) registrar todos os acessos ou tentativas de acesso de um dispositivo ao SERVIÇO, mantendo o registro mesmo na hipótese de desativação do uso ou descadastramento de um dispositivo;

e) impedir que um usuário, a partir de um dispositivo hierarquicamente inferior, *i.e.*, cujo cadastramento tenha ocorrido por último, descadastre um dispositivo hierarquicamente superior, *i.e.*, cujo cadastramento tenha ocorrido primeiro;

f) impedir que um usuário, a partir de um dispositivo hierarquicamente inferior, *i.e.*, cujo cadastramento tenha ocorrido por último, desabilite a Invenção;

iv. Para o primeiro acesso de um usuário previamente identificado onde não há dispositivos cadastrados:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) o Servidor de Autenticação verifica o parâmetro listado no item ***ii. "a"***;

c) o Servidor de Autenticação verifica os parâmetros listados nos itens ***ii. "c"*** e ***"d"***.;

d) com base na anuência do usuário, a ASSINATURA é cadastrada, o dispositivo é incluído no grupo autorizado e o usuário tem acesso ao SERVIÇO;

e) se o item ***"b"*** acima não for satisfeito, o acesso ao SERVIÇO é negado;

v. Para os acessos subseqüentes de um usuário previamente identificado a partir de um dispositivo já cadastrado:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) o Servidor de Autenticação reconhece a ASSINATURA, autorizando o acesso ao SERVIÇO em caso de sucesso;

vi. Para os acessos subseqüentes de um usuário a partir de um dispositivo não cadastrado:

a) o Agente Coletor cria uma ASSINATURA para o dispositivo conforme descrito na reivindicação 1;

b) O Servidor de Autenticação verifica os parâmetros listados no item ***ii "a"*** e ***"b"***; e,

c) aplicam-se as etapas descritas nos itens ***iv "c"*** e ***"d"***;

d) se o item ***"b"*** acima não for satisfeito, o acesso ao SERVIÇO é negado.

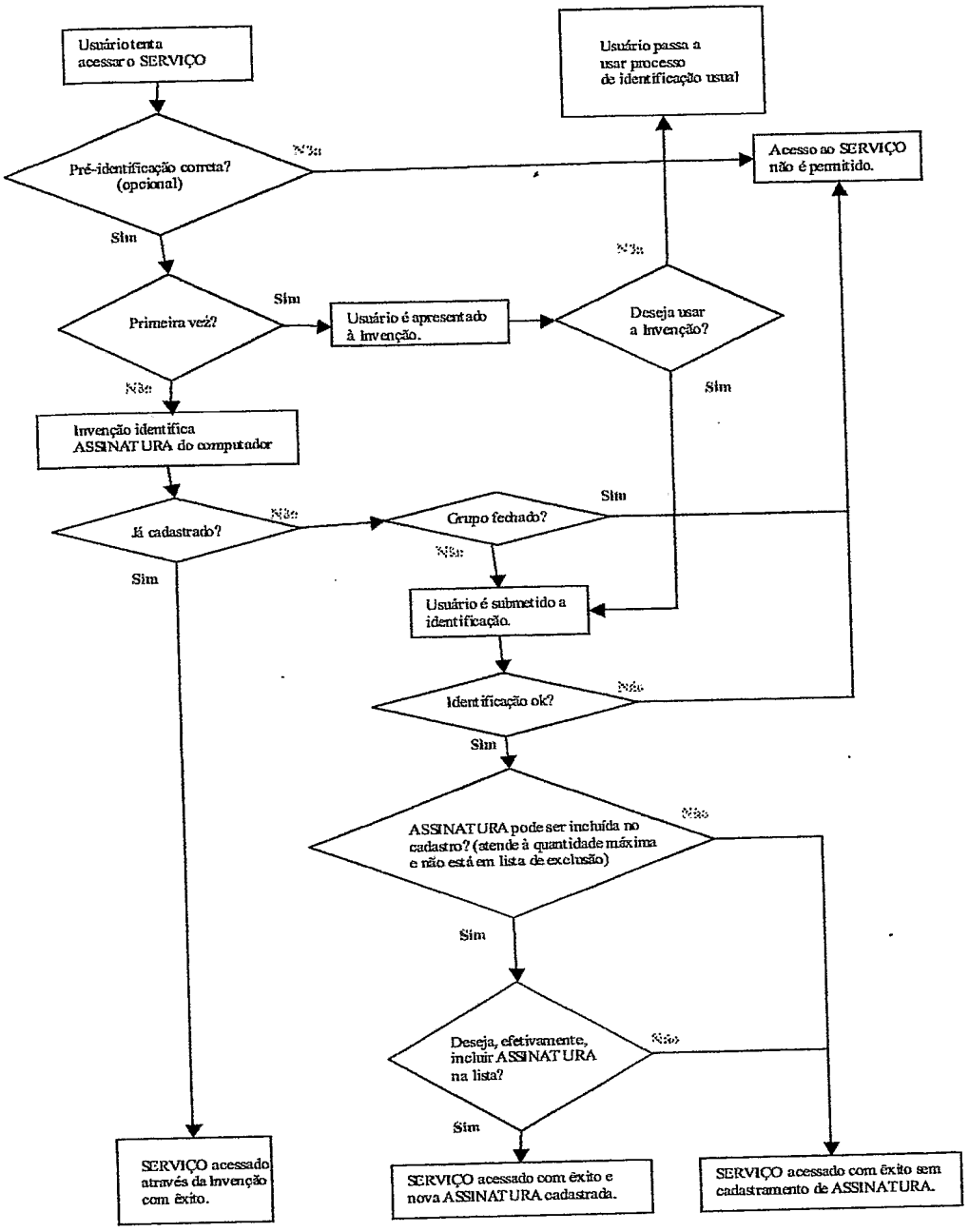


FIG. 1

Obs. Nas figuras 1, 2 e 3, O termo "Identificação" se refere à positivação estendida.

FIG. 2

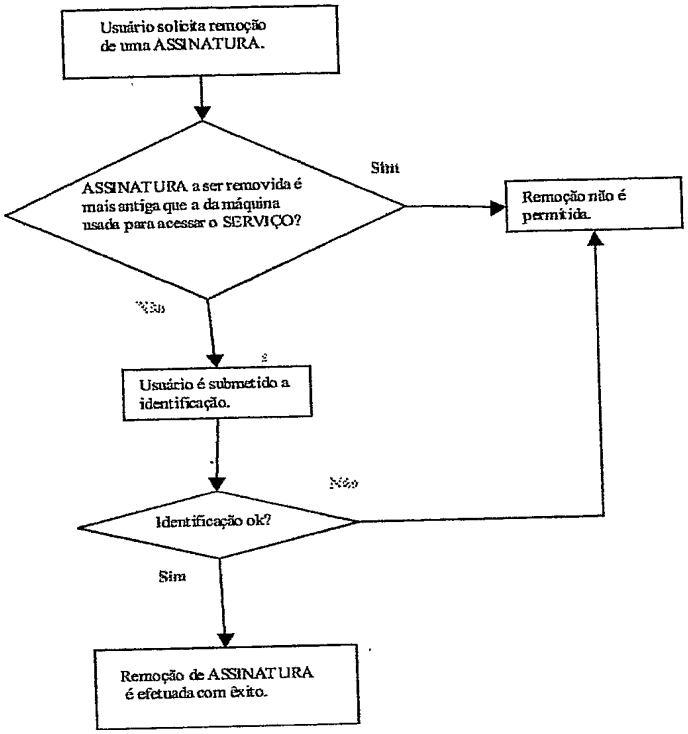
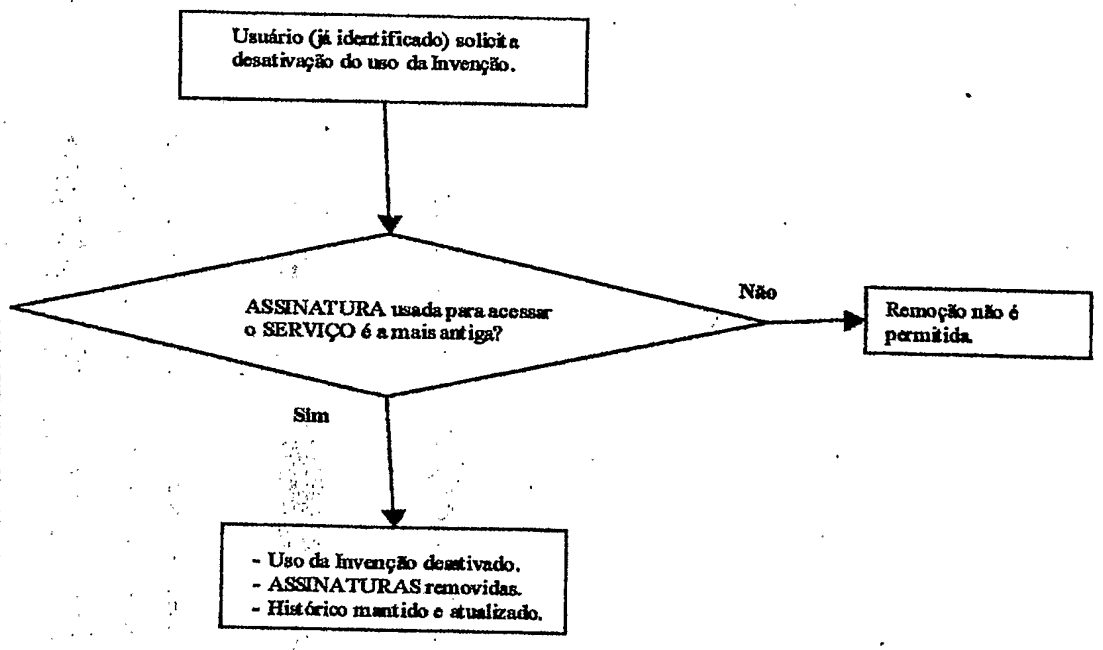

Usuário solicita remoção de uma ASSINATURA.
ASSINATURA a ser removida é mais antiga que a da máquina usada para acessar o SERVIÇO?
Sim
Não
Remoção não é permitida.
Usuário é submetido a identificação.
Não
Identificação ok?
Sim
Remoção de ASSINATURA é efetuada com êxito.

FIG. 3


Usuário (já identificado) solicita desativação do uso da Invenção.
ASSINATURA usada para acessar o SERVIÇO é a mais antiga?
Não
Remoção não é permitida.
Sim
- Uso da Invenção desativado.
- ASSINATURAS removidas.
- Histórico mantido e atualizado.

SISTEMA DE CONTROLE DE ACESSO A SERVIÇOS DE INFORMAÇÃO BASEADO EM ASSINATURA DE HARDWARE E SOFTWARE DO DISPOSITIVO SOLICITANTE

A presente Invenção refere-se a dispositivos computacionais ou com capacidade computacional para identificação e autenticação de acesso.

Mais particularmente, a presente Invenção é aplicada no acesso a informações sensíveis e confidenciais tais como acessos via internet a contas bancárias, acesso seguro a páginas eletrônicas para transações comerciais (*e-commerce*), acesso a intranet de uso confidencial em ambientes empresariais, etc.